International Journal of English Literature and Social Sciences
Vol-9, Issue-3; May-Jun, 2024

Peer-Reviewed Journal
Journal Home Page Available: https://ijels.com/
Journal DOI: 10.22161/ijels

Factors Affecting the Implementation of Cybersecurity in the Philippine Coast Guard

Leopoldo DG Apillanes Jr.

Received: 30 Mar 2024; Received in revised form: 04 May 2024; Accepted: 12 May 2024; Available online: 21 May, 2024

Abstract— *This study investigates the factors influencing the implementation of cybersecurity in the Philippine Coast Guard (PCG) to ensure national security and maritime safety. The research focused on policies, circulars, developmental plans, equipment, and human resources. A mixed-methods approach was used, collecting quantitative data through a survey of 90 MARSLEC personnel to assess their cybersecurity awareness and perceptions of current measures. Qualitative insights were obtained from in-depth interviews with deputy commanders of MARSLEC units. The results revealed key obstacles: unclear policies and circulars, limited budget and resources for cybersecurity equipment, and insufficient specialized training and skilled personnel. Despite these challenges, there was a strong commitment from PCG leadership to prioritize cybersecurity. Effective collaboration with other agencies and organizations was deemed crucial. The study recommended addressing these challenges by clarifying policies, optimizing resource allocation, and implementing continuous training and awareness programs. By improving cybersecurity readiness, the PCG could better safeguard national interests, maritime assets, and personnel against evolving cyber threats. These measures are essential for enhancing the PCG's cybersecurity posture and ensuring resilient maritime operations.*

Keywords— ***Cybersecurity, Philippine Coast Guard, Mixed-Methods, Training, Policy Implementation***

I. INTRODUCTION

Background of the Study

Cybersecurity is critical in safeguarding the maritime operations of the Philippine Coast Guard (PCG). With increasing cyber threats, the PCG's Maritime Security and Law Enforcement Command (MARSLEC) must adopt robust cybersecurity measures. This study examines the factors affecting cybersecurity implementation within the PCG, focusing on policies, resources, and training.

Statement of the Problem

This study aimed to identify the factors affecting the implementation of cybersecurity in the PCG. Specifically, it answered the following questions:

1. What is the demographic profile of MARSLEC personnel concerning cybersecurity?
2. What is the level of awareness in Cybersecurity of MARSLEC personnel in terms of laws, best practices, and threats?
3. How is Cybersecurity implemented in MARSLEC in terms of policies, equipment, and human resources?
4. Is there a significant relationship between the demographic profile and the level of awareness on Cybersecurity of MARSLEC personnel?
5. What are the factors that affect the implementation of Cybersecurity in MARSLEC?
6. What capacity training program can be proposed based on the findings of the study?

Significance of the Study

This study provides valuable results that can contribute to the advancement of cybersecurity in the maritime sector.

Specifically, the following stakeholders may benefit from this research:

1. **Philippine Coast Guard**: Develop and enhance cybersecurity measures to protect critical infrastructure and operational systems from cyber threats.
2. **Department of Transportation (DOTr):** Promote interagency collaboration, enhance cyber risk management, and ensure legal and regulatory cybersecurity frameworks in safeguarding transportation infrastructure.
3. **Future Researchers**: Contribute to knowledge advancements, support risk assessment, and collaboration in the field of cybersecurity.

Scope and Delimitations

This study identified the factors affecting the implementation of cybersecurity in the PCG, specifically within MARSLEC units. The investigation combined quantitative and qualitative methodologies to provide a holistic view of cybersecurity implementation factors.

II. INTEGRATED RELATED LITERATURE AND STUDIES (IRLS)

Cybersecurity in Maritime Operations

Maritime cybersecurity is a growing concern globally. According to BIMCO (2021), guidelines on cybersecurity onboard ships highlight the critical need for robust security measures to protect maritime operations. The National Institute of Standards and Technology (2018) emphasizes the importance of a comprehensive cybersecurity framework to address vulnerabilities and threats.

Factors Influencing Cybersecurity Implementation

Research by Marble et al. (2015) identifies key factors affecting cybersecurity implementation, including policy clarity, resource allocation, and training. The study indicates that unclear policies and inadequate resources can significantly hinder cybersecurity efforts.

Training and Awareness Programs

Effective cybersecurity awareness training is crucial for enhancing cybersecurity readiness. Canepa et al. (2021) stress the importance of comprehensive training programs tailored to the specific needs of maritime personnel. Chew (2023) further highlights the role of continuous training in maintaining high levels of cybersecurity awareness.

Interagency Collaboration

Collaborative efforts are essential in strengthening cybersecurity measures. The ReCAAP Information Sharing Centre (2021) underscores the benefits of information sharing and interagency cooperation in combating maritime cyber threats.

Cybersecurity in the Philippine Coast Guard

The PCG's cybersecurity policy, as outlined in Circular No. 11-19 (Philippine Coast Guard, 2019), sets the framework for cybersecurity measures within the organization. However, the implementation of these policies faces challenges, including limited budget and resources (Cabanlong, 2019).

Technological Adoption in Maritime Operations

Understanding the acceptance of cybersecurity measures within maritime operations is essential. Dwivedi et al. (2019) utilize the Unified Theory of Acceptance and Use of Technology (UTAUT) to explore factors influencing technology adoption, providing insights into the adoption behavior of maritime personnel.

III. METHODS

Research Design

A convergent mixed-methods design was used, integrating quantitative surveys and qualitative interviews. This approach provides a comprehensive understanding of cybersecurity implementation within MARSLEC.

Conceptual Framework

The conceptual framework of this study integrates the Input-Process-Output (IPO) model with principles derived from the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) see Figure 1. This alignment focuses on the factors of cybersecurity acceptance and adoption in the PCG, particularly within MARSLEC.

Input Phase: Drawing from TAM and UTAUT, the study gathers various variables, including demographic data, academic backgrounds, cybersecurity training, and previous assignments of MARSLEC personnel. It assesses their awareness levels regarding cybersecurity laws, regulations, best practices, and threats, and examines existing cybersecurity practices, encompassing policies, circulars, reports, developmental plans, software, hardware, and human resources.

Process Phase: Aligned with UTAUT, this phase evaluates the perceived ease of engaging in cybersecurity practices among PCG personnel. Survey questionnaires assess personnel perceptions of adopting and implementing cybersecurity measures, while interview questionnaires gain in-depth insights into challenges and facilitators of cybersecurity practices. This phase also examines the

impact of social norms and influential figures within MARSLEC on cybersecurity adoption and implementation.

Output Phase: This phase focuses on facilitating conditions, reflecting elements from both TAM and UTAUT. It involves proposing a tailored capacity training program on cybersecurity for MARSLEC, addressing specific needs and challenges identified. Recommendations are made for improving resource allocation and strategies to foster a culture of cybersecurity awareness and compliance within the PCG.

Figure 1: IPO Model

Input	Process	Output
- MARSLEC Unit's Personnel - Demographic Information - Level of awareness in cybersecurity - MARSLEC implementation of cybersecurity - Factors affecting the implementation of cybersecurity in PCG applied in MARSLEC	- Survey Questionnaire - Interview Questionnaire	- Capacity training program on cybersecurity for MARSLEC - Recommendations for Resource Allocation - Strategies to Foster a Cybersecurity Culture

Respondents

The study involved 90 MARSLEC personnel for the survey and four deputy commanders for interviews. Participants were selected using purposive sampling to ensure relevant insights.

Ethical Considerations

Informed consent was obtained from all participants, and confidentiality was maintained. The study adhered to ethical guidelines set by the Philippine Merchant Marine Academy (PMMA).

Instrumentation

1. **Survey Questionnaire**: A four-part survey questionnaire assessed demographic profiles, awareness levels, cybersecurity implementation, and influencing factors. The scale options ranged from 'fully unaware' to 'fully aware' and from 'strongly disagree' to 'strongly agree.'
2. **Interview Questionnaire**: Semi-structured interviews elicited detailed responses about practical aspects of cybersecurity implementation, challenges, and training programs.

Validation of Instrument

Both instruments underwent validation. The survey questionnaire was pretested and reliability was confirmed using Cronbach's Alpha. The interview questionnaire was validated through face and content validity.

Data Gathering Procedure

Survey data were collected via Google Forms, and interviews were conducted online or face-to-face. Data were securely stored and prepared for analysis.

Data Analysis

Quantitative data were analyzed using descriptive statistics and Pearson correlation coefficients. Qualitative data were transcribed and thematically analyzed to provide insights into cybersecurity implementation and challenges.

IV. RESULTS

Demographic Profile

Age: The majority (58.89%) were aged 20-30 years. This indicates a trend of younger individuals being involved in cybersecurity within the PCG.

Age	Frequency	Percentage (%)
20 to 30 years old	53	58.89
31 to 40 years old	28	31.11
41 to 50 years old	8	8.89
over 50 years old	1	1.11
Total	**90**	**100.00**

Sex: Predominantly male (70%), reflecting the current gender composition within cybersecurity roles.

Sex	Frequency	Percentage (%)
Male	63	70.00
Female	27	30.00
Total	90	100.00

Rank: Majority were non-officers (83.33%), suggesting that non-officer personnel are more engaged in day-to-day cybersecurity tasks.

Rank & Current Position/ Designation	Frequency	Percentage (%)
Officers	**15**	**16.67**

CG Security Border Protection Service	4	26.67
CG Investigation, Detection, Management Service	3	20.00
CG K9 Force	3	20.00
CG Sea Marshal Force	3	20.00
CG Surface Patrol Force	2	13.33
Non-Officers	**75**	**83.33**
CG Sea Marshal Force	20	26.67
CG K9 Force	20	26.67
CG Security and Border Protection Service	13	17.33
CG Investigation, Detection, and Management Service	12	16.00
CG Surface Patrol Force	8	10.67
CG Security Border Protection Service	2	2.67
Total	**90**	**100.00**

Years in Service: Most had 1-5 years of service (40%), highlighting a relatively new workforce.

Years in Service	Frequency	Percentage (%)
Less than 1 year	14	15.56
1 to 5 years	36	40.00
6 to 10 years	21	23.33
More than 10 years	19	21.11
Total	**90**	**100.00**

Academic Background: Predominantly Bachelor's degree holders (74.44%).

Academic Background	Frequency	Percentage (%)
Bachelor's Degree Holder	67	74.44
Master's Degree Holder	1	1.11
Others	22	24.44
Total	**90**	**100.00**

Cybersecurity Training: A significant gap in training, with 93.33% having not received formal training.

Cybersecurity Training Received	Frequency	Percentage (%)
Yes	6	6.67
No	84	93.33
Total	**90**	**100.00**

Previous Cybersecurity Duties: Only 1.11% had previous cybersecurity roles, indicating limited prior exposure.

Previous Assignment to Cybersecurity Duties	Frequency	Percentage (%)
Yes	1	1.11
No	89	98.89
Total	**90**	**100.00**

Awareness Levels

Pertinent Laws and Regulations: Overall mean awareness level of 2.50 (Aware), with highest awareness for the Data Privacy Act of 2012 and the Anti-Photo and Video Voyeurism Act of 2009.

PERTINENT LAWS, RULES, AND REGULATIONS (CIRCULARS, POLICIES, ETC.)	MEAN	VI
Data Privacy Act of 2012 (Republic Act No. 10173)	2.67	Aware
Anti-Photo and Video Voyeurism Act of 2009 (Republic Act No. 9995)	2.67	Aware
Cybercrime Prevention Act of 2012 (Republic Act No. 10175)	2.64	Aware
Utilization of PCG Provided Email Services (SOP No. 05-19)	2.58	Aware

Policy Guidelines to Raise Security, Awareness, Consciousness, and Discipline on the Use of Information and Communications Technology (ICT) Devices and the Internet of PCG Personnel (Circular 09-14)	2.53	Aware
Implementing Rules and Regulations of the Data Privacy Act	2.51	Aware
Utilization of Issued PCG Mobile / Cellular Phones (SOP No. 19-19)	2.49	Unaware
Department of Information and Communications Technology (DICT) Act of 2015 (Republic Act No. 10844)	2.49	Unaware
Philippine Coast Guard Cybersecurity Policy (Circular No. 11-19)	2.42	Unaware
National Cybersecurity Plan 2023 (NCSP 2023)	2.34	Unaware
Electronic Commerce Act of 2000 (Republic Act No. 8792)	2.32	Unaware
Government Procurement Reform Act (Republic Act No. 9184)	2.30	Unaware
OVERALL MEAN	**2.50**	***Aware***

Legend: 3.25 – 4.00 — Fully Aware; 2.50 – 3.24 — Aware; 1.75 – 2.49 — Unaware; 1.00 – 1.74 — Fully Unaware; VI – Verbal Interpretation

Best Practices: Overall mean awareness level of 2.93 (Aware), with highest awareness for using strong passwords, maintaining physical security, and securing Wi-Fi networks.

BEST PRACTICES ON CYBERSECURITY	MEAN	VI
Use strong and unique passwords	3.24	Aware
Maintain physical security	3.13	Aware
Secure Wi-Fi networks	3.10	Aware
Regularly back up data	3.04	Aware
Keep software up to date	2.98	Aware
Use reputable antivirus software	2.98	Aware
Educate employees on the awareness of best practices in cybersecurity	2.90	Aware
Limit user privileges	2.89	Aware
Be cautious of phishing attempts	2.86	Aware
Conduct regular security assessments	2.86	Aware
Develop an incident response plan	2.86	Aware
Encrypt sensitive data	2.84	Aware
Implement multi-factor authentication (MFA)	2.81	Aware
Implement a firewall	2.80	Aware
Regularly monitor and analyze logs	2.71	Aware
OVERALL MEAN	**2.93**	***Aware***

Legend: 3.25 – 4.00 — Fully Aware; 2.50 – 3.24 — Aware; 1.75 – 2.49 — Unaware; 1.00 – 1.74 — Fully Unaware; VI – Verbal Interpretation

Cybersecurity Threats: Overall mean awareness level of 2.62 (Aware), with highest awareness for phishing, password attacks, and e-commerce fraud.

CYBERSECURITY THREATS	MEAN	VI
Phishing	2.83	Aware
Password Attacks	2.78	Aware
E-commerce and Payment Card Fraud	2.76	Aware
Malware	2.69	Aware
Social Engineering	2.68	Aware
Ransomware	2.67	Aware
Insider Threats	2.66	Aware
Data Breaches	2.63	Aware

Internet of Things (IoT) Threats	2.56	Aware
Cryptojacking	2.56	Aware
Denial of Service (DoS) Attack	2.54	Aware
Advanced Persistent Threats (APTs)	2.53	Aware
Distributed Denial of Service (DDoS) Attacks	2.52	Aware
Structured Query Language (SQL) Injection	2.50	Aware
Man-in-the-Middle (MitM) Attacks	2.49	Unaware
Zero-day Exploits	2.46	Unaware
OVERALL MEAN	**2.62**	***Aware***

Legend: 3.25 – 4.00 — Fully Aware; 2.50 – 3.24 — Aware; 1.75 – 2.49 — Unaware;

1.00 – 1.74 — Fully Unaware; VI – Verbal Interpretation

Implementation of Cybersecurity

Policies and Documentation: Overall mean implementation level of 2.50 (Implemented), with significant awareness but gaps in specific internal policies.

INDICATORS	MEAN	VI
MARSLEC has development plan on cybersecurity	3.00	Agree
MARSLEC makes guidelines or SOPs in cybersecurity	2.98	Agree
MARSLEC conducts webinars or seminars to promote cybersecurity awareness.	2.94	Agree
MARSLEC sends reiteration of policies, circulars, documentary reports and/or developmental plan on a continuing basis	2.90	Agree
Infographics about cybersecurity is disseminated to MARSLEC personnel	2.88	Agree
OVERALL MEAN	**2.94**	***Agree***

Legend: 3.25 – 4.00 — Strongly Agree; 2.50 – 3.24 — Agree; 1.75 – 2.49 — Disagree;

1.00 – 1.74 — Strongly Disagree; VI – Verbal Interpretation

Equipment: Overall mean implementation level of 2.93 (Implemented), indicating a good understanding of best practices but room for improvement in regular monitoring and multi-factor authentication.

INDICATORS	MEAN	VI
MARSLEC provides computer hardware components {i.e. Central Processing Unit (CPU), Random Access Memory (RAM), Hard Disk Drive (HDD), Graphics Processing Unit (GPU), Network Interface Card (NIC)}	2.94	Agree
MARSLEC provides standard software (i.e. Firewall Tools, Antivirus, Web Vulnerability Scanning Tools, Application Software)	2.84	Agree
MARSLEC has offices to cater cybersecurity issues.	2.77	Agree
MARSLEC uses variety of modalities (physical, virtual, blended, etc.) to cater to the stakeholders and general public in terms of cybersecurity concerns.	2.74	Agree
OVERALL MEAN	**2.83**	***Agree***

Legend: 3.25 – 4.00 — Strongly Agree; 2.50 – 3.24 — Agree; 1.75 – 2.49 — Disagree;

1.00 – 1.74 — Strongly Disagree; VI – Verbal Interpretation

Human Resources: Overall mean implementation level of 2.62 (Implemented), with identified need for increased training and awareness programs.

Human Resources (skills, training, etc.)	Mean	VI
MARSLEC personnel is sent for cybersecurity-related trainings.	2.86	Agree
Presence of MARSLEC personnel in every PCG districts with cybersecurity related duties	2.76	Agree
MARSLEC personnel's cybersecurity performance are evaluated on a regular basis.	2.71	Agree
OVERALL MEAN	**2.77**	***Agree***

Legend: 3.25 – 4.00 — Strongly Agree; 2.50 – 3.24 — Agree; 1.75 – 2.49 — Disagree;

1.00 – 1.74 — Strongly Disagree; VI – Verbal Interpretation

Factors Affecting Implementation

Policy Clarity: Unclear policies hinder effective implementation, highlighting the need for simplified and well-disseminated policies.

Resources: Limited budget and equipment constrain cybersecurity efforts, emphasizing the need for optimized resource allocation.

Training: Insufficient specialized training impacts readiness, underscoring the importance of continuous training programs.

V. DISCUSSION

Policy Clarity and Dissemination

The study found that unclear policies significantly hinder effective cybersecurity implementation. Simplified and well-disseminated policies are crucial for ensuring that all personnel are aware of and can comply with cybersecurity protocols. This aligns with Vaidya's (2019) research, which emphasizes the importance of targeted awareness campaigns and training initiatives to ensure understanding and compliance with cybersecurity regulations.

Resource Allocation

The limited budget and resources for cybersecurity equipment were identified as major obstacles. Optimizing resource allocation to provide adequate funding for cybersecurity infrastructure and tools is essential. This finding is supported by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which highlights the need for continuous assessment and updates to technological infrastructure to mitigate cybersecurity risks.

Training and Development

The study highlighted a significant gap in specialized cybersecurity training among MARSLEC personnel. Continuous training and development programs are crucial for enhancing cybersecurity readiness. This is in line with Canepa et al. (2021) and Chew (2023), who emphasize the importance of comprehensive cybersecurity awareness training within the maritime domain.

Interagency Collaboration

Effective collaboration with other agencies and organizations was highlighted as crucial. Partnerships with governmental bodies such as the Department of Information and Communications Technology (DICT) can enhance cybersecurity skills and address evolving cyber threats. The ReCAAP Information Sharing Centre's annual report underscores the benefits of information sharing and collaboration in combating maritime cyber threats.

Regulatory and Legal Challenges

The implementation of the National Cybersecurity Strategy Framework by the DICT represents a significant step toward addressing regulatory and legal challenges. Ensuring swift adaptation to changing regulations and integrating these into the cybersecurity strategy is essential. Developing agile regulatory adaptation processes can ensure compliance and effectiveness.

Cyber Risk Management

In the maritime industry, cyber risk management involves adapting to continuous security evolution to manage cyber risks effectively. This includes technical measures, strategic planning, senior management involvement, and continuous risk assessment to address vulnerabilities and threats dynamically.

Adoption and Use of Technology

Understanding the acceptance of cybersecurity measures within the PCG is essential for ensuring a secure operational environment. Evaluating personnel perceptions and adoption of cybersecurity practices using models like the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) provides insights into technology acceptance and usage behavior.

Recommendations

1. **Policy Clarification**: Simplify and disseminate clear cybersecurity policies.
2. **Resource Optimization**: Allocate adequate budget and resources for cybersecurity infrastructure.
3. **Continuous Training**: Implement ongoing training programs to improve skills and awareness.
4. **Enhanced Collaboration**: Foster interagency collaboration to leverage shared knowledge and resources.
5. **Agile Regulatory Adaptation**: Develop processes to swiftly adapt to changing cybersecurity regulations.

VI. CONCLUSION

Enhancing the PCG's cybersecurity readiness requires addressing policy, resource, and training challenges. By implementing the recommended measures, the PCG can better protect its maritime operations from evolving cyber threats. This study provides actionable insights that contribute to strengthening the cybersecurity resilience of MARSLEC and the PCG as a whole.

ACKNOWLEDGEMENTS

Special thanks to the PCG, MARSLEC personnel, and PMMA faculty for their support. Gratitude to my family for their unwavering encouragement.

REFERENCES

[1] BIMCO. (2021). Guidelines on cybersecurity onboard ships.
[2] Cabanlong, J. (2019). National cybersecurity plan 2022.
[3] Canepa, G., et al. (2021). Comprehensive cybersecurity awareness training in the maritime domain. Journal of Maritime Security, 12(3), 45-59.
[4] Chew, S. (2023). Developing effective cybersecurity awareness training programs. Cybersecurity Journal, 15(2), 101-112.
[5] Cyber Assurance of Physical Security Systems (CAPSS). (2024). Cybersecurity measures. CAPSS Annual Report, 2024.
[6] Cyber Risk GmbH. (n.d.). Cyber risk management in the maritime industry. Retrieved from https://www.cyberriskgmbh.com.
[7] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.
[8] DayBlink Consulting. (2019). Structuring an organization's cybersecurity team. DayBlink White Paper Series.
[9] Department of Information and Communications Technology. (2017). National cybersecurity plan 2022.
[10] Department of Information and Communications Technology. (2019). National cybersecurity strategy framework.
[11] Dwivedi, Y. K., et al. (2019). Adoption and use of technology in the maritime industry: A UTAUT perspective. International Journal of Maritime Technology, 5(1), 23-37.
[12] Elev8. (2024). The importance of cybersecurity awareness training for employees. Elev8 Cybersecurity Insights, 2024.
[13] International Maritime Organization. (2022). IMO regulation on cybersecurity measures. IMO Maritime Safety Committee, Resolution MSC.428(98).
[14] International Organization for Standardization. (2022). ISO/IEC 27001: Information security management systems.
[15] Marble, C., et al. (2015). Cybersecurity vulnerabilities in maritime operations. Journal of Cybersecurity Research, 8(4), 213-229.
[16] National Institute of Standards and Technology. (2018). NIST cybersecurity framework.
[17] Nobles, J. (2018). Human factors in cybersecurity: A maritime perspective. Journal of Maritime Security, 11(2), 88-99.
[18] Philippine Coast Guard NHQ-PCG/CG-11 Circular No. 11-19. (2019). PCG cybersecurity policy.
[19] Philippine Coast Guard NHQ-PCG/CG-11 Standing Operating Procedures No. 05-19. (2019). Utilization of PCG provided email services.
[20] Philippine Coast Guard NHQ-PCG/CG-11 Standing Operating Procedures No. 09-19. (2019). Utilization of issued PCG mobile/cellular phones.
[21] Philippine Coast Guard HPCG Circular No. 09-14. (2014). Policy guidelines to raise security awareness, consciousness, and discipline on the use of ICT devices and the internet of PCG personnel.
[22] Philippine Coast Guard CGWCEISC. (2021). PCG cybersecurity corps.
[23] Philippine Merchant Marine Academy. (2023). Factors affecting the implementation of cybersecurity in the Philippine Coast Guard.
[24] Punzalan, R. (2017). Technological dependencies and regulatory challenges within the PCG. Journal of Maritime Policy and Management, 14(2), 98-114.
[25] ReCAAP Information Sharing Centre. (2021). Annual report on piracy and maritime cyber threats.
[26] Securities and Exchange Commission. (2020). Cybersecurity framework for regulated entities. SEC Bulletin, 2020(5), 45-58.
[27] Turyahumura, J. (2021). Global collaboration in maritime cybersecurity. International Maritime Security Journal, 18(3), 134-147.
[28] University of the Philippines Diliman. (2019). Data Privacy Act of 2012 (Republic Act No. 10173).
[29] Uy, A. (2023). Cybersecurity definition and scope. Journal of Information Security, 10(1), 22-31.